特権IDログ監査の現実的・効率的な運用
―「SecureCube /Access Check」のゲートウェイ型アプローチ―

昨今、重要サーバーにアクセスできる特権IDを使った情報漏えい事件が増えていることから、特権IDのログ監査への注目が高まっている。本稿では、NRIセキュアテクノロジーズの特権ID管理ソリューション「SecureCube /AccessCheck」の紹介を通じて、厳格な特権ID管理のためのログ監査のポイントについて解説する。

重要性を増す特権IDのログ監査

高い権限を有するrootやAdministratorなどの特権IDを不正に利用した情報漏えい事件が増加していることを受けて、特権IDに対する注目が強まっている。特権IDの管理は、IT全般統制の観点で金融当局や監査法人が重視するポイントでもあり、金融庁が公表している「金融検査指摘事例集」でも「顧客保護等管理態勢」の不備として取り上げられている。クレジットカード業界のグローバルセキュリティ基準「PCI DSS」でも、一定規模の加盟店が準拠認定を求める場合に、重要サーバーへのアクセス状況のログ監査が必須要件とされている。こうしたことから、昨今では情報セキュリティの大きな課題として特権ID管理に注目が集まっているのである。

特権IDのログ監査の難しさ

一般に、情報漏えいの早期発見と迅速な対処のためには、最初にアクセスログの確認が必要とされる。特にセキュリティ事故の原因究明においては、操作ログが最有力の手掛かりとなる。誰がどんな操作をしたかという記録である。

まず、情報システムにログインできるアカウントには、権限を限定された個別のIDと、高度な権限を付与された特権IDがある。一般の開発者・運用者に対して担当業務を遂行するために割り振られる個別IDは、その悪用を防ぐために、決められたポリシーに従って定期的にパスワードを変更してセキュリティレベルを高めているのが一般的である。

一方で、特別な作業のために必要となる特権IDは、システムへの影響を考慮して定期的なパスワードの変更ができないことが多い。そのため、補完的な統制として利用者を限定して運用しているケースがある。

この場合、複数の開発者や運用者が特権IDとパスワードを共有することが多く、操作ログをすべて取得していたとしても、誰が操作を行ったかを特定するのは困難である。また、特権IDは全ての高度な権限を持つため、取得したログの削除や改ざんも可能である。従って、厳格な特権ID管理のためには、特権IDの利用者からログ管理権限を分離し、第三者がログ監査を行うようにすることが求められる。

実際に行われている対策としては、①作業内容に応じて、重要サーバーへのアクセスの

NRIセキュアテクノロジーズ
セキュリティソフトウェア事業本部
セキュリティソフトウェア事業二部
上級セキュリティコンサルタント
岸　謙介（きしけんすけ）
専門は情報セキュリティシステム全般

都度、暫定的な特権IDを発行する②各サーバーに、必要な権限のみを付与した開発者・運用者の個人IDを割り振る③全ての重要サーバーにアクセス管理ツールやログ管理ツールを導入する–などがある。しかし、システムの規模が拡大してサーバーの台数が増えるほど作業量や費用が増大する。そのため、課題として認識していても、このような対策も実施できていない事例は少なくない。

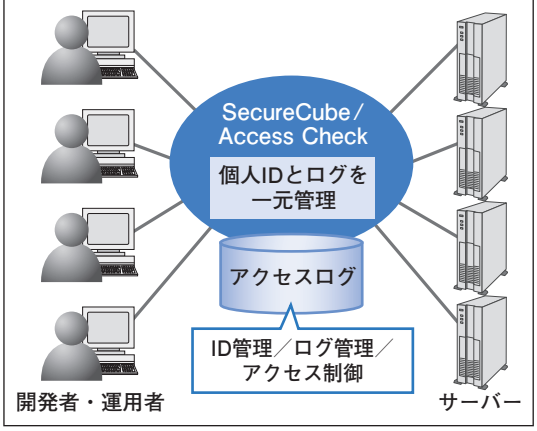
特権IDログ監査システムの導入が不可欠

前述のとおり、特権IDのログ監査においては「特権ID利用者の特定」と「特権ID利用者とログ監査者との権限分離」が重要なポイントとなる。しかし開発や運用の現場では、ログ確認のポイントが曖昧になりがちで、また特権ID利用者とログ監査者が一緒になって不都合なログを削除や改ざんするなどの不正を行う可能性も否定できない。そのため、開発・運用とは別の組織を設け、第三者が統一された一定の基準でログを監査する体制を構築することが求められる。これらを全て人手で行うには限界があり、現実的で効率的な運用のためにはシステムの導入は避けられない。

有効なゲートウェイ型アプローチ

NRIセキュアテクノロジーズでは、前述した課題を解決するために「SecureCube / Access Check」を利用したゲートウェイ型アプローチを提案している（図1参照）。

図1　ゲートウェイ型の特権ID管理のイメージ



開発者・運用者と重要サーバーとの間にゲートウェイを設置し、ここに個人を識別するIDを登録する。開発者・運用者が重要サーバーへアクセスする際は、個別IDでゲートウェイへログインしたのち、重要サーバー上で共用されている特権IDと個別IDを関連付ける。これにより、誰がどこにアクセスして何をしたかという、利用者を特定したログ監査の仕組みをゲートウェイ上で実現できる。

ゲートウェイという性質上、操作ログは重要サーバーとは別のサーバーに保管されることになるため、特権ID利用者によるログの改ざんは困難である。また、必然的に複数サーバーのログの一元管理ができるようになるため、作業の効率化や監査精度の向上といった効果も期待できる。対象の重要サーバーが増加した場合にシステムコストや運用コストが大きく増加しない点もゲートウェイ型の大きなメリットである。■